

STAVERTON PARISH COUNCIL

Data Protection Policy

ADOPTED ON *draft*

- **Introduction**

Staverton Parish Council is fully committed to compliance with the requirements of the Data Protection Act 1998 (“the Act”), which came into force on the 1st March 2000. The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act.

- **Policy statement**

In order to operate efficiently, The Parish Council has to collect and use information about people within the parish and with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act to ensure this.

Staverton Parish Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it communicates. The Council will ensure that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

- **The principles of data protection**

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **'sensitive' personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

- **Handling of personal/sensitive information**

Staverton Parish Council will, through appropriate management and the use of criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply checks to determine the length of time information is held;
- Take appropriate measures to safeguard personal information;

- **Disclosure to Third Parties**

Personal Data, including email addresses, must not be disclosed to a Third Party without the express agreement of the persons concerned and only in accordance with the provisions of the Data Protection Act.

- **Access Rights By Individuals**

An individual may request a copy of any data held about them, or information about the reason it is kept or processed and the people to whom it is disclosed. The information must be provided, in clearly understandable terms within 40 days of a valid written request and the payment of any required fee.

A person seeking information shall be required to prove their identity in accordance with the Data Protection Act. The 40 days will run from the date the person provides this information, and pays any required fee.

Information may be withheld where the Council is not satisfied that the person requesting information about themselves are who they say they are, or when the requester is an organisation or body requesting information on behalf of a named individual and the Council is not satisfied that they have the authority to receive that information.

If an individual complains that the data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime a note should be made on the person's 'file' indicating that there is a query over the data accuracy and this should remain in place until the matter is resolved.

- **Violations of Rules & Procedures**

It is the responsibility of all councillors to report any suspected breaches of the Data Protection Act, or of this Policy, to the Clerk.

Failure to comply with this Data Protection Policy by employees of Council may result in disciplinary action being taken. Failure to comply by Councillors may constitute a breach of The Members' Code of Conduct. Failure to comply by partners, agents or contractors may constitute a breach of their agreements.

- **Complaints**

Any complaint or concern expressed by an individual in connection with the Data Protection Act must be reported to the Clerk immediately. The Clerk will determine if there has been a breach of the Act and present their findings to the Council to decide what action, if any, needs to be taken.

- **Notification to the Information Commissioner**

The Information Commissioner enforces and oversees the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOI). The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. The Information Commissioner keeps a register of all organisations, which process data. If required, the Council shall submit a Notification to the Information Commissioner and pay the requisite fee at least once a year, which will be dealt with by The Clerk. Members and staff of Council must furnish The Clerk with any information requested for this purpose. Members and staff of Council must notify The Clerk if, during the course of any year, this information changes, and The Clerk must update the Register entry accordingly. Members may have to register personally with the Information Commissioner with respect to constituency or party records.

The Policy will be reviewed annually.